전력분석공격에 대한 실험환경 분석

강영진* · 이훈재**

*동서대학교 유비쿼터스 IT학과

**동서대학교 컴퓨터정보공학부

Experimental Environment Analysis for Power Analysis Attacks

Young Jin Kang* · Hoon Jae Lee**

*Dept. of Ubiquitous IT, Dongseo University Graduate School

**Div. of Computer Information Engineering, Dongseo University

E-mail : rkddudwls55@gmail.com, hjlee@dongseo.ac.kr

요 약

현재 정보보호에 대한 중요성이 부각되고 있으며 u-Korea 또는 유비쿼터스 IT 시대에서는 정보보호가 더욱 중요시 되고 있으며, 특히 소형 암호 장치에 있어서 핵심이 되는 암호 알고리즘의 보안성이 중요한 부분이지만 전력분석공격은 암호 알고리즘 자체의 안전성이 높다고 하더라도 암호 알고리즘이 구현된 방법이나 구현된 환경에 따라 적용이 가능한 공격이다. 이에 본 논문에서는 전력분석공격에 대하여 설명하고, 실험환경을 분석 하고자 한다.

ABSTRACT

The importance of this emerging information security and u-Korea or ubiquitous IT era, and the information security is more important. Especially, the small core device password encryption algorithm is an important part of the secure side channel attack cryptographic algorithms. However, it can provide high level of security, an adversary can attack small core device through implementation of cryptographic algorithms. In this paper describes for the Power Analysis attack and analyze the experimental environment.

키워드

Side Channel Attacks, PA Attack, Hamming weight,

Ⅰ. 서 론

부채널 공격은 암호 알고리즘의 이론적인 취약점이 아닌 암호화 과정에서 누설되는 타이밍 정보, 전력, 전자파 신호등을 이용한 공격이다. 또한 정보 보호에 대한 중요성이 부각되고 있으며, u-Korea 또는 유비쿼터스 IT 시대에서는 정보보호가 더욱 중요시 되고 있으며, 암호장치가 대중화 되고 있는 추세이다. 암호 장치에 있어서 암호 알고리즘은 핵심이라 할 수 있고, 이에 암호 알고리즘의 보안성이 중요한 부분이며, 암호 알고리즘을 공격하여 키 값 등의 중요한 정보를 탈취하려는 행위에 노출되어 있으며, 부채널 공격에 위협받고 있다.

부채널 공격 중 가장 강력한 공격에 속하는 전력분석공격은 크게 단순전력분석(SPA, Simple Power Analysis), 차분전력분석(DPA, Differential Power Analysis), 상관전력분석(CPA, Correlation Power Analysis) 기법으로 나누어지며, 알고리즘이 구현된 방법 또는 환경에 따라 적용이 가능한 공격기법이다[1-2].

본 논문에서는 전력분석공격에 대하여 살펴보고, 일반적인 전력분석 실험환경에 대하여 분석하고자한다.

Ⅱ. 전력분석공격

전력분석공격은 P.Kocher 등이 제안한[1-2] 공

격기법이다.

암호 알고리즘은 암호문과 비밀키의 상관도가 매우 낮도록 설계되어, 알려진 평문과 암호문을 이용하여 비밀키를 찾는 것은 매우 어렵다. 그래서 그림 1에서 보는 바와 같이 알고리즘 진행 중에 식(1)과 같이 알려진 값(P_t)과 알려지지 않은 비밀 중간키 값(k_t)을 입력으로 연산하며, 알려진 값(P_t)과 연산결과 값(c_t)의 상관도가 매우 높은 특정시점(t)를 선정하여 공격한다. 식(1)에서 P_t는 알고 있으나 c_t를 알 수 없어 k_t의 추정이 불가능하므로, c_t가 생성될 때 소모하는 전력신호(T_t)를 c_t대신 사용한다. 전력분석 공격은 선정된 특정시점(t)에서 가능한 가지 수의 k_t로부터 추정된 전력신호(h_t)들과 측정된 전력신호(T_t) 사이의 상관도를 분석하여 공격하는 방법이다.

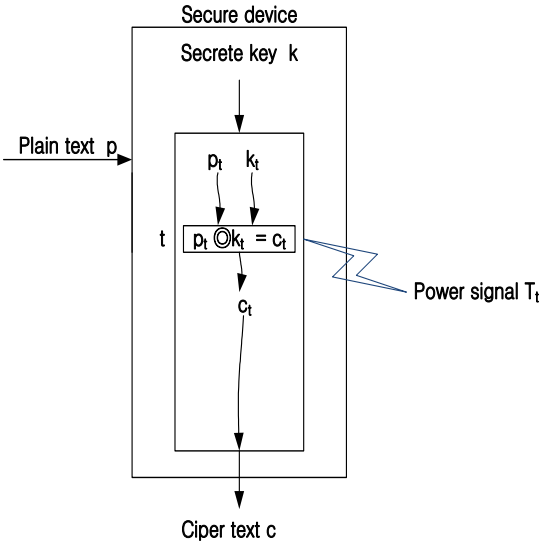

그림 1. 전력분석공격[3]

$$c_t = p_t \odot k_t \quad (1)$$

전력분석공격은 다음의 4 단계를 거쳐서 공격하게 된다.

- 1단계 : 전력신호 측정

암호 알고리즘을 분석하여 암호알고리즘 실행 중에 알려진 값(P_t)과 비밀 중간키(k_t)가 연산하는 적절한 공격시점(t)를 선택하고, 전력신호(T_t)를 측정한다.

- 2단계 : 연산 값 추정

공격시점(t)에서 가능한 모든 비밀 중간키(k_{ti})를 가정하고, 각각의 비밀 중간키(k_{ti})에 대하여 연산 값(c_{ti})를 추정한다. 여기서 8비트 연산 시스템인 경우 k_{ti}는 256가지 (i=0, ... , 255)이다.

- 3단계 : 소모 전력 추정

추정된 연산 값(c_{ti})을 이용하여 공격 시점에서의 소모전력을 추정(h_{ti})한다.

- 4단계 : 통계적 상관도 분석

h_{ti}와 T_t의 통계적 상관도를 분석하면, 올바르게 추정된 h_{ti}에 대하여는 높은 상관계수 값을 가지게 되고, 잘못 추정된 h_{ti}에 대하여는 낮은 상관계수 값을 가지게 되어 비밀 중간키(k_{ti})를 찾을 수 있다. 찾은 비밀 중간키(k_{ti})를 이용하여 비밀키(k)를 추정 계산한다.

III. 실험환경 분석

3.1 전력분석공격의 실험환경

전력분석공격의 실험환경은 아래의 그림 2과 같이 먼저 암호 모듈을 오실로스코프와 연결한다. 그리고 측정된 소모전력 신호를 수집하기 위해 PC와 연결하고 암호 모듈에 평문과 암호화를 실행시키기 위해 암호모듈과 PC를 연결한다.

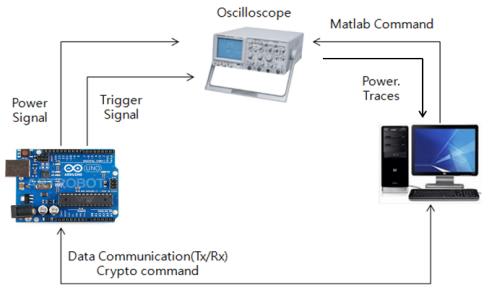

그림 2. 전력분석공격 실험 환경 구성도

3.2 소모전력 신호 측정

서로 다른 평문을 이용하여 소모전력을 신호를 측정한다. 그림 3은 측정되는 소모전력 신호이며, 아래의 신호는 트리거 신호로 공격 시점을 나타낸다. 또한 위의 신호는 실제 측정하고 수집하는 소모전력 신호이다.

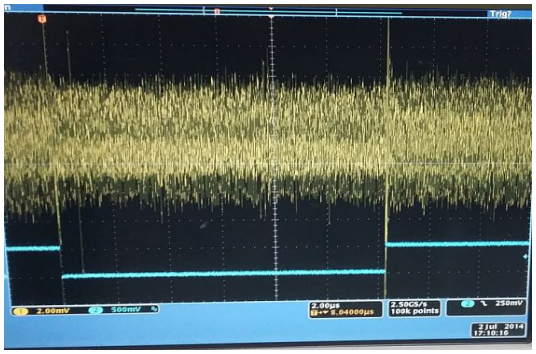

그림 3. 공격시점에서의 소모전력 신호

3.3 추측 키 생성

추측 키 생성을 하기에 앞서 '공격 대상을 AES 암호알고리즘, 공격시점을 AddRoundKey로 가정을 한다'. 그리고 3-2에서 사용한 평문을 이용하여 추측키를 생성한다. p_{ji}를 평문이라 할 때 j는 평문의 수 i는 해당 바이트 위치라고 하면, 각 p_j의 i번째 값에 대해서 가능한 모든 경우의 키를 AddRoundKey연산을 수행하여 추측 키 테이블을 생성한다.

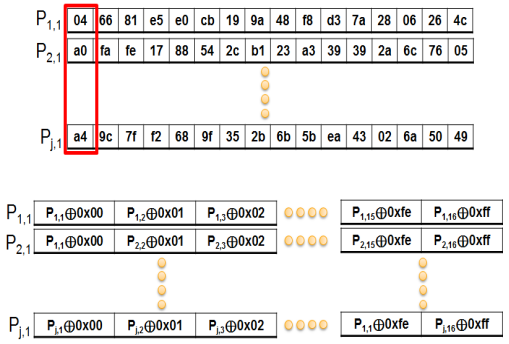

그림 4. 추측 키 생성 과정

생성한 추측 키 테이블을 해밍 무게 모델을 사용하여 추정 전력 값 테이블을 생성한다. 해밍 무게 모델은 데이터 버서를 통과하는 어떠한 값의 '0'과 '1'의 개수에 따라 전력의 크기가 다르다는 모델로 '1'이 많을수록 많은 전력을 소모한 것으로 '1이 많을수록 측정된 신호는 작다. 아래의 그림 5는 해밍 무게 모델을 나타내며, 식(2)는 추측 키를 해밍 무게 모델로 바꾸는 식을 나타낸다.

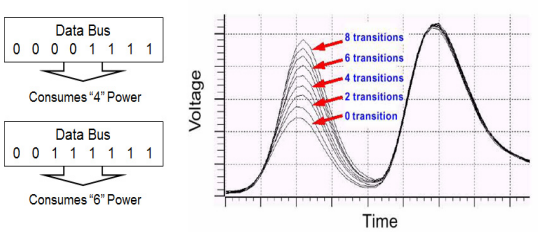

그림 5. 해밍 무게 모델

$$HW(P_{j,i} \oplus (00 \ldots 255)) \qquad (2)$$

이처럼 위의 과정(3.1 ~ 3.3)을 가지고 추정된 소모전력 값과 측정된 전력신호 사이의 상관계수들을 계산하면 상관계수 추정 값을 찾을 수 있다[4].

Ⅳ. 결 론 및 향후 계획

현재 부 채널 공격은 시스템의 취약점을 찾아 공격하는 현실적인 공격기법으로 인식되고 있으며, 이와 같은 기반으로 안전한 암호 시스템을 구축하는데 좋은 도구로 이용되고 있다.

본 논문에서는 Kocher의 전력분석공격이 어떻게 이루어지는가에 대하여 살펴보았다. 또한 전력분석공격의 실험을 위해 실험환경을 분석하였으며, 향후 분석한 데이터를 가지고 전력분석공격 실험을 통해 결과 값을 제시하고자 한다.

감사의 글

이 논문은 2013년 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었다. (과제번호:2013-071188)

참고문헌

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of Advances in Cryptology-CRYPTO'99, pp. 388-397, Springer-Verlag, 1999.

[2] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," http://www.cryptography,com/dpa/technical, 1988.

[3] 박영구, 김형락, 이훈재, 한덕찬, 박의영, "비밀 중간키를 이용한 소프트웨어적 전력분석공격 방어대책," 한국정보통신학회논문지, Vol. 17, No. 12, 2013.12.

[4] Young Jin kang, Tae Yong kim, Jung Bok Jo, and Hoon Jae Lee, "An Experimental CPA attack for Arduino Cryptographic Module and Analysis in Software-based CPA Countermeasures," International Journal of Security and Its Applications, pp. 261-270, Vol. 8, No. 2, 2014.